

FTK ENTERPRISE 7.5.1

RELEASE NOTES

October 2021

Table of Contents

Overview3

1 New Features & Enhancements3

2 Resolved Issues..... 15

3 Known Issues 17

Contact Exterro..... 18

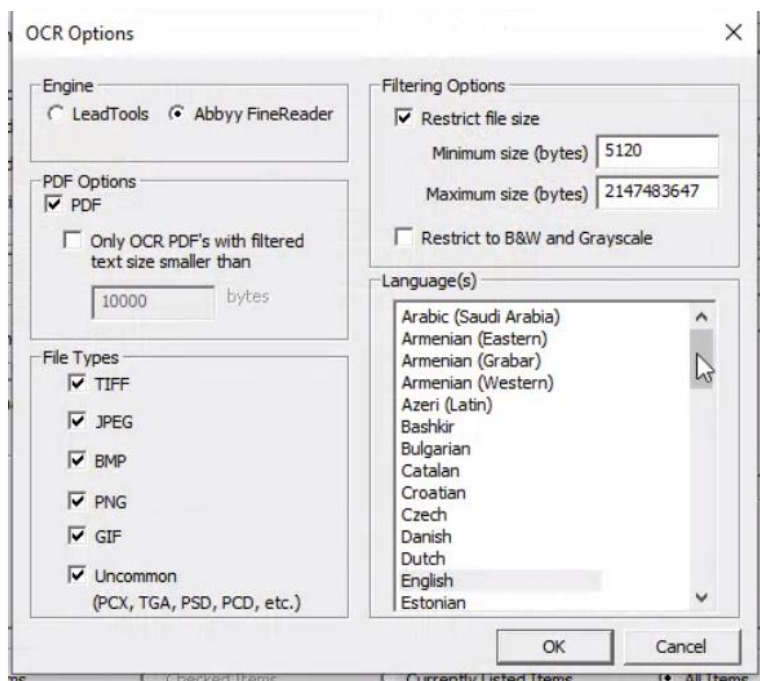
Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Legal GRC platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

1 New Features & Enhancements

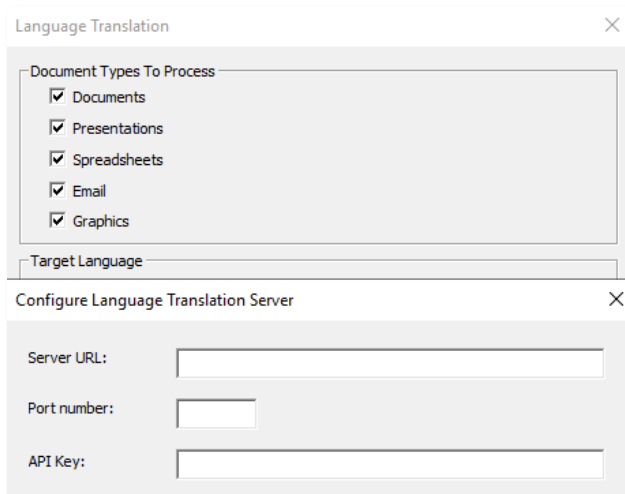
1. FTK now supports ABBYY FineReader OCR engines in addition to LeadTools.

Note: Refer to ABBYY installation and configuration in this KB [article](#). (Contact sales@exterro.com for more information). (FCR-894)



2. FTK has been enhanced to allow Offline Language Translation:

- RWS Offline Language Translation is now supported for (FCR-1234):
 - Documents
 - Presentations
 - Spreadsheets
 - Email
 - Graphics



If you have an active RWS SDL license, language identification and translation can be enabled within FTK and FTK Plus.

Note: Refer to RWS installation and configuration in this KB [article](#). (Contact sales@exterro.com for more information).

3. FTK has been given performance enhancements:

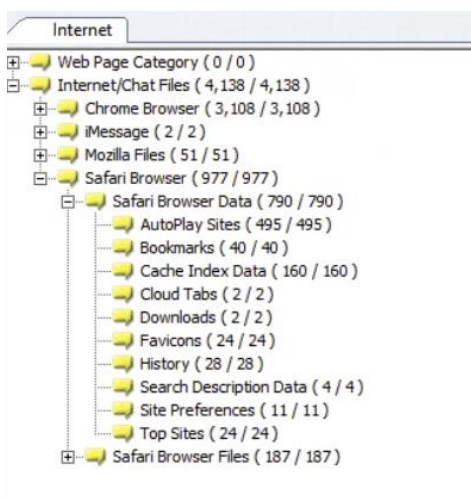
- Case Loading Times have been reduced. (FCR-1100)
- Improved Processing Speeds for ZIP files. (FCR-1062)
- Improved Processing Speeds for MBOX files. (FCR-801)
- Improved Indexing Speeds. (FCR-590)
- Improved Speed when Opening Cases for the first time in FTK after a user has logged out and then logged in. (FCR-1545)

4. FTK supports ingestion and processing of Virtual Machine Backups (FCR-1482) (FCR-57):

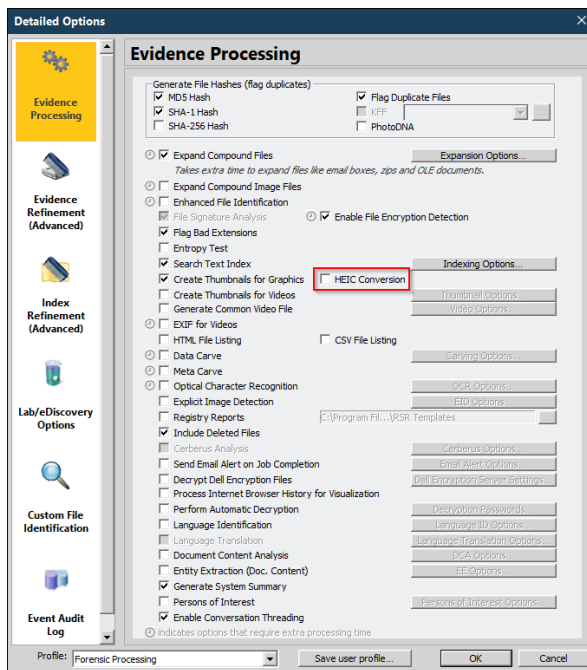
- VDI
- VMDK
- VHD
- VHDX

5. FTK has been enhanced to parse/process/view new OS X artifacts:

- **Browser Data and Browser Files from Safari.** (FCR-804)
 - AutoPlay Sites
 - Downloads
 - Site Preferences
 - AutoFill Correction Files
 - Cloud AutoFill Files
 - Downloads File
 - Site Preferences
 - Cloud Tabs
 - History
 - Top Sites
 - Cache Index Files
 - Cloud Tabs File
 - History File
 - Top Sites File



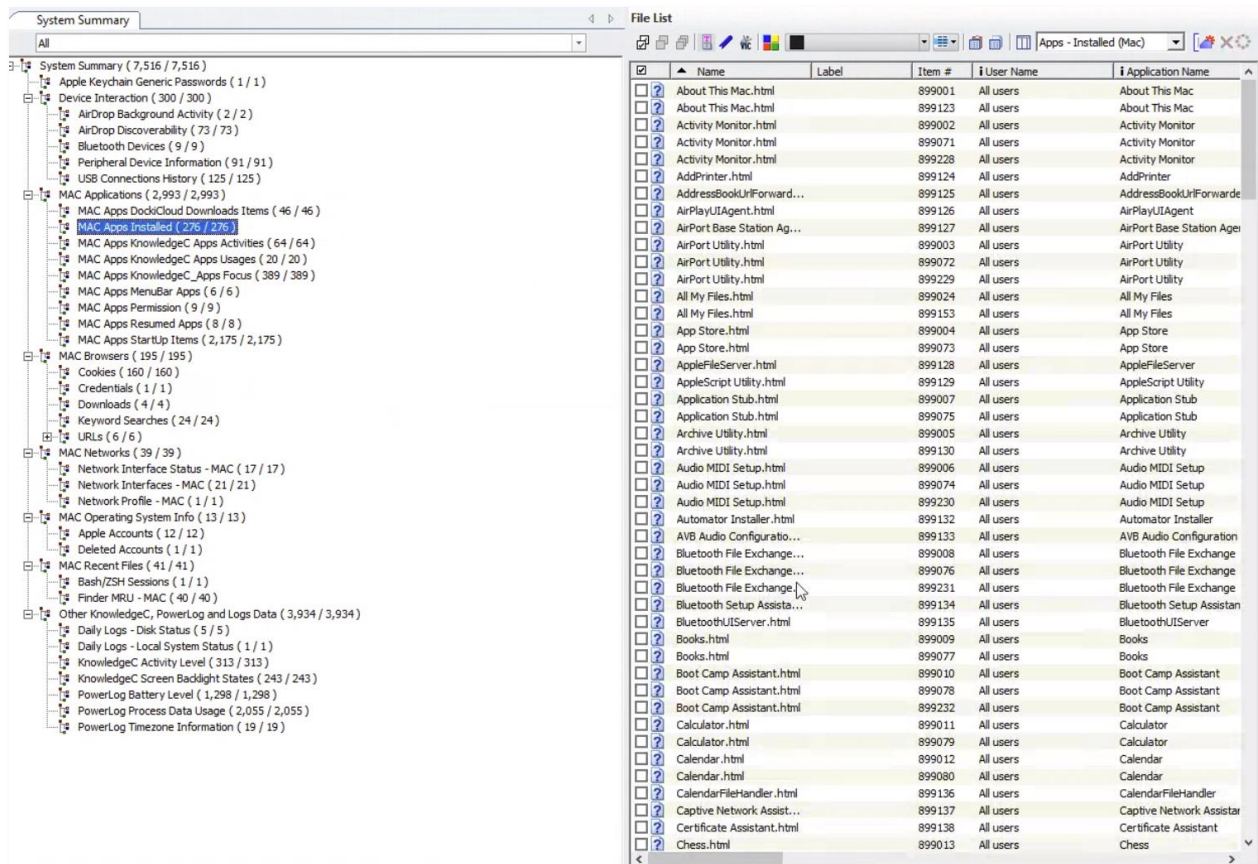
- **HEIC Images** – A new processing option, “HEIC Conversion” has been added to support native review of HEIC images in FTK. (FCR-21)



- **iWork 10.13 (and later) documents** – Users can now review iWork files natively in FTK Plus and FTK Central. While FTK cannot do this natively, it can view the resultant files within the viewer once conversions have completed. (FCR-40)

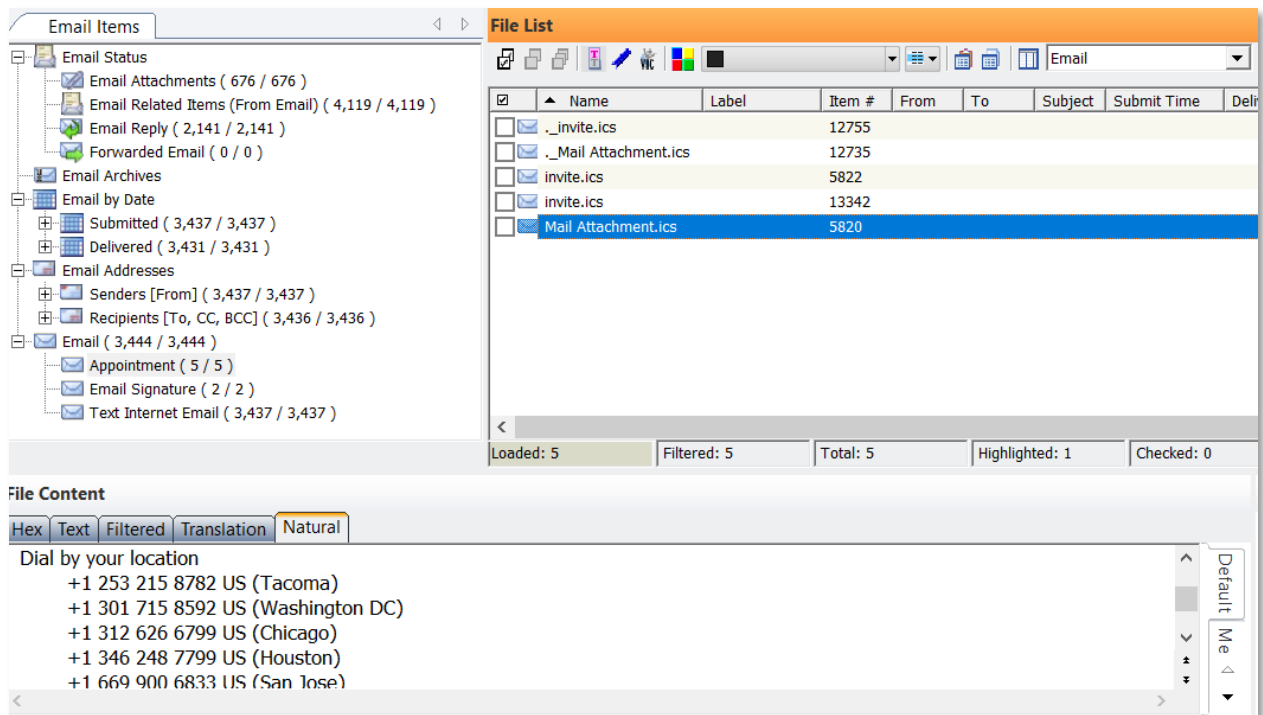
Note: Refer to the View iWork Files in FTK Plus/Central using this KB [article](#). Refer to Viewing iWork Files in this KB [article](#).

- **OS X System Information** – By using the existing the “Generate System Summary” processing option, OS X system information can be viewed in the System Summary tab. Associated column sets can be found in the OS Information column group. Refer to the full list of supported OS X System Information in this KB [article](#) (FCR-1210) (FCR-2056)

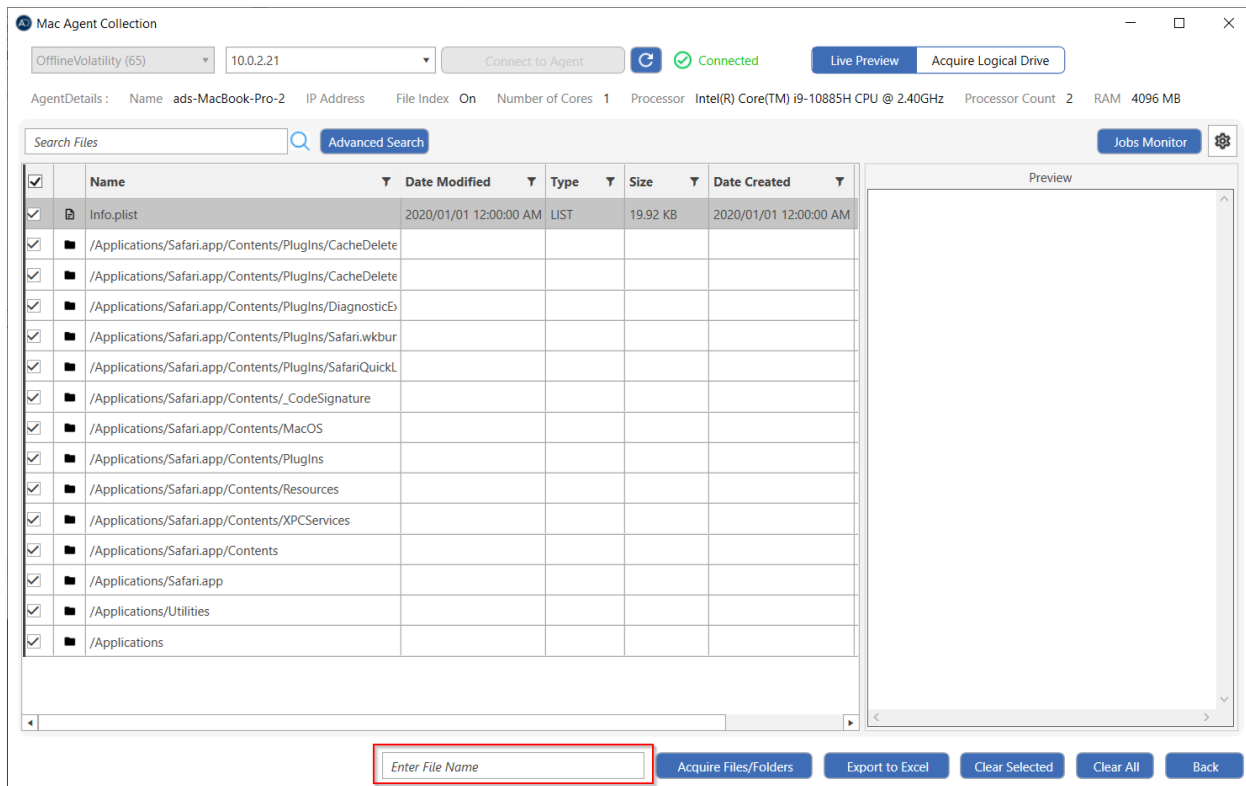


- **Outlook for Mac** – FTK now supports parsing of emails from Outlook for Mac (2012 – 2019). OLK/OLM formats change constantly and hence If your OLK version is not parsed as expected, please contact support@exterro.com. (FCR-1151)

- **EMLX** – EMLX files are now fully supported to parse and display Email signatures, appointments and attachments appropriately in the Email tab. (FCR-41)



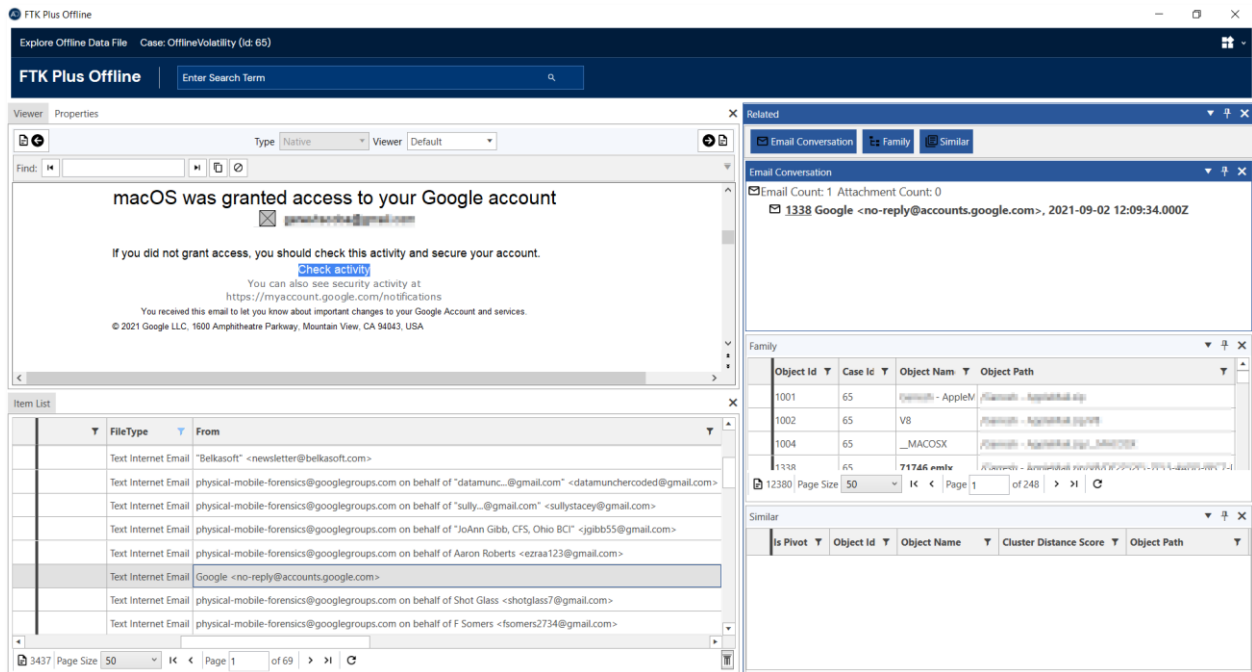
- **Mac Agent has been given performance/optimization enhancements:**
- **Port Default** – The Agent is now configured to run on port 3999 by default. (FCR-440)
- **Customized Collection Name** – Mac Agent collections can now be given a customized name. Previously, all OS X collections were automatically named after its GUID. (FCR-462)



- **Resource Consumption Optimizations** – The agent no longer utilizes all available resources during collections. (FCR-1815)

6. Portable Cases have been enhanced:

- **Family Panel** – Portable cases now feature the Related panel with Email Conversations, Family and Similar. (QR-978)



- **Last Used Export Paths** – While trying to perform an export in a portable case, the “Export Path” field will be auto-populated with the folder path that was used for the previous export operation. (FCR-638)
- **Customized Layouts** – During portable case creation, customized layouts are now exported with the case. (FCR-631)
- **Case Names** – Case names will now be displayed while reviewing a portable case. (FCR-629)
- **Application Scaling** – Files present in a portable case will now be automatically scaled to fit your screen. (FCR-636)

7. You can now edit the names of screen captures present in FTK reports. (FCR-589)



8. FTK has been enhanced to further parse/process the following artifacts:

- Windows Event Logs** – Event logs are now categorized in the System Summary tab. (FCR-584)
 - Remote Desktop Protocol
 - Account Management Events
 - Shared Objects Events
 - Audit Policy Change Events
 - PowerShell Events
 - Process Tracking
 - Other Events
 - Power Events
 - Login/Logout events
 - Scheduled Task Events
 - Windows Service Events
 - Wireless LAN Auditing Events
 - USB Mass Storage Events

The screenshot displays the FTK Enterprise 7.5.1 interface. The top pane shows the 'System Summary' tab with a tree view of system artifacts. The bottom pane shows the 'File Content' tab with a list of Windows Event Logs.

System Summary Tree View:

- System Summary (130,778 / 130,778)
 - Applications (2,140 / 2,140)
 - Device Interaction (81 / 81)
 - Networks (23 / 23)
 - Operating System Info (1,622 / 1,622)
 - Recent Files (1,112 / 1,112)
 - Windows Events (119,702 / 119,702)
 - Account Management Events (1,549 / 1,549)
 - Audit Policy Change Events (2,948 / 2,948)
 - Login/Logout events (4,309 / 4,309)
 - Other Windows Events (102,284 / 102,284)
 - Process Tracking (4,806 / 4,806)
 - Remote Desktop Protocol (3,212 / 3,212)
 - Scheduled Task Events (284 / 284)
 - Shared Objects Events (293 / 293)
 - Windows Service Events (17 / 17)
 - Windows SRUM Events (6,098 / 6,098)

File Content Tab - Event Record Details:

EventRecordID	1000
Correlation	
Execution	
[ProcessID]	680
[ThreadID]	8300
Channel	Microsoft-Windows-Winlogon/Operational
Computer	DESKTOP-746K5BU
Security	
[UserID]	S-1-5-21-2157821824-2741069011-2528395153-1001
EventData	<EventData> <Data Name="Event">12</Data> <Data Name="SubscriberName">Sens</Data> </EventData>

File List Tab - Event Log Entries:

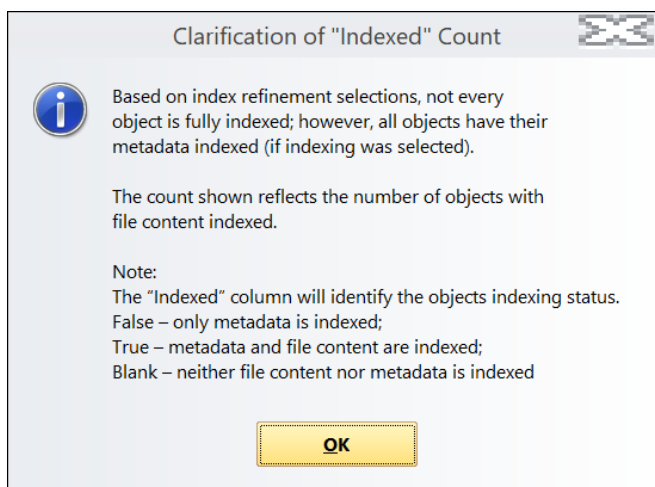
Name	Label	Item #	Event ID	Task Category	Event Src	Event Level	Created	Description	Path	Category
event #1		325547	551	Logoff	Microsoft-Windows-SMB...	2	7/19/2019 9:32...		Win10.E01/OS64 [NTFS...	Login/...
event #10		3237613	812	Special Logon	Microsoft-Windows-Win...	4	6/23/2019 11:3...		Win10.E01/OS64 [NTFS...	Login/...
event #100		3239403	812	Special Logon	Microsoft-Windows-Win...	4	6/24/2019 7:02...		Win10.E01/OS64 [NTFS...	Login/...
event #1000		3240653	812	Special Logon	Microsoft-Windows-Win...	4	7/7/2019 12:36...		Win10.E01/OS64 [NTFS...	Login/...
event #10001		3285864	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10003		3285866	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10005		3285868	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10007		3285870	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10008		3285871	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10009		3285872	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10012		3285875	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10014		3285877	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10016		3285879	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10018		3285881	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #1002		3240655	812	Special Logon	Microsoft-Windows-Win...	4	7/7/2019 12:36...		Win10.E01/OS64 [NTFS...	Login/...
event #10020		3285883	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10022		3285885	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10024		3285887	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10026		3285889	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10028		3285891	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10030		3285893	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10032		3285895	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10034		3285897	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...
event #10036		3285899	4624	Logon	Microsoft-Windows-Sec...	0	7/19/2019 9:34...		Win10.E01/OS64 [NTFS...	Login/...

loaded: 4,309 | Filtered: 4,309 | Total: 4,309 | Highlighted: 1 | Checked: 0 | Click to update size

- **Additional Chrome User Activity Databases** – Additional user activity databases are now categorized. (FCR-857)
 - Web AutoFill Data
 - Current Session Data
 - Last Session Data
 - Last Tabs
 - Sync Accounts
 - Saved Credit Cards

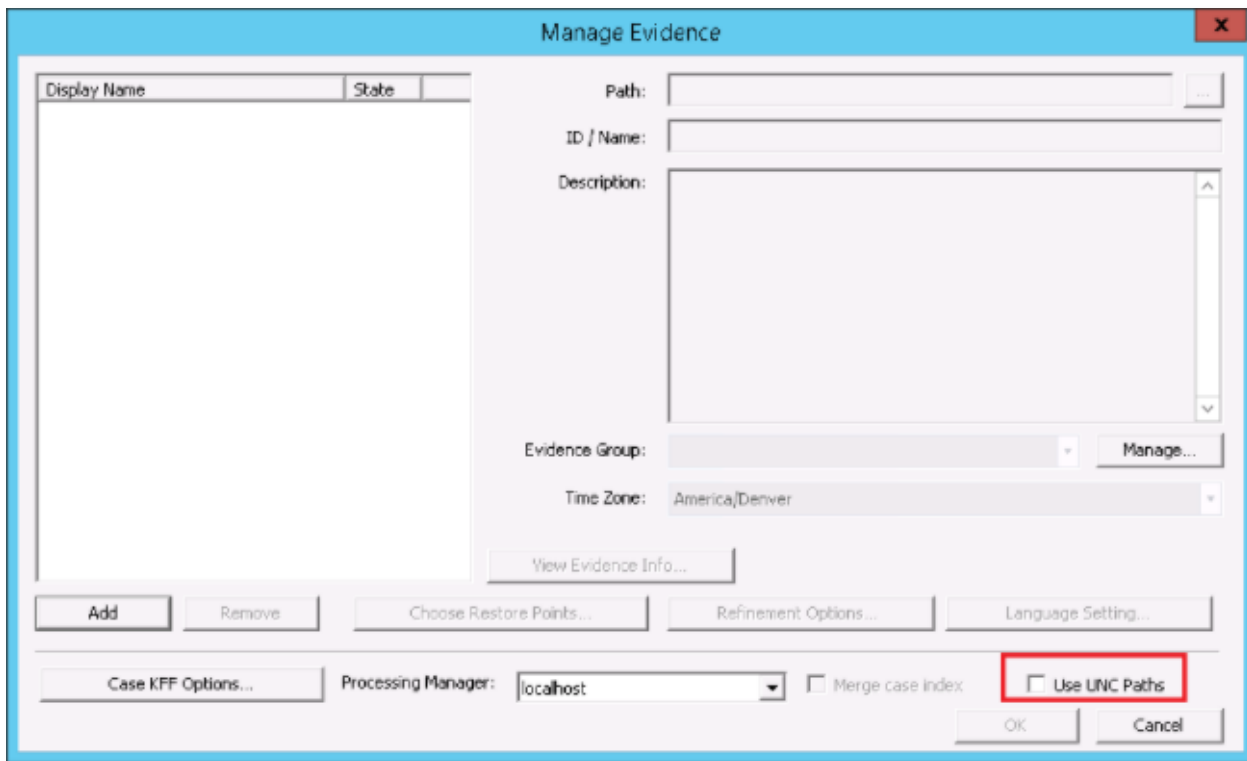
9. Indexing changes & enhancements:

- **@ Symbol Inclusion** – The @ symbol is now indexed by default and is listed among the characters in the processing profile Indexing Options dialog. (FCR-160)
- **Underscores Indexed as Space** – Underscores are indexed as a space character by default. Words in text that are joined by an underscore will be indexed as two separate words by default. (FCR-103)
- **Forensic Processing Profile** – This processing profile has been updated to not index slack space and unallocated space to ensure quicker initial processing times. However, users can index unindexed objects by utilizing Additional Analysis.



10. Chats within a PST are now parsed for visualization in Chat view. (FCR-800)

11. FTK Column groups are now categorized to allow for efficient viewing. The default column groups available are: (FCR-1086)
- Common
 - Email
 - Internet
 - Location
 - Media
 - Mobile
 - Reports
 - Summary Information
12. During application upgrades, you will be prompted with an upgrade dialogue to accept or decline the database upgrade if applicable. (FCR-724)
13. The “Use UNC Path” in the Manage Evidence popup is now enabled by default for the FTK Lab and Enterprise applications (FCR-1697)





14. DBConfig is enhanced to improve security and stability:

- **Migration Options** – This option has been removed due to compatibility issues. (FCR-1360)
- **Custom Settings** – This option is removed to ensure case databases are stored separately. (FCR-1360)
- **Optimization Settings** – This option is removed due to compatibility issues. (FCR-1360)
- **Internal Authentication Methods and Passwords** – Using the lock icon, authentication methods and passwords can be updated. (FCR-130)
- **SA Account** – The account is no longer a requirement to initialize the SQL database. Any account that has the “sysadmin” server-level role, can be used for initialization of the database. (FCR-1824)



2 Resolved Issues

1. Resolved an issue where Skype desktop chat messages were not displayed in the 'Mobile data' tab (FCR-1281)
2. Resolved an issue where Windows 10 Pro event log files (EVTX) were not parsed during evidence processing. (FCR-708)
3. Resolved an issue where Apple Mail attachments were not displayed in email attachments when the contents were processed from the Directory. (FCR-1273)
4. Resolved an issue where Apple MBOX email attachment contents were not visible in the viewer. (FCR-665) (FCR-61)
5. Resolved an issue where the PST files were not processed when the evidence was chosen from 'Contents of a Directory' (FCR-1244)
6. Resolved an issue where some multi-page PDF files were sporadically not OCR'd. (FCR-1110)
7. Resolved an issue where FTK did not parse the required information from AFF4 images and USB devices (FCR-1275) (FCR-1283)
8. Resolved an issue where Virtual hard disk (VHD) image files from the VirtualBox files were not processed (FCR-1295)
9. Resolved an issue where ADprocessor.exe consumed all the available RAM when a OneNote file was encountered in evidence for processing. (FCR-2071)
10. Resolved an issue where large UFED Physical Analyzer Report Package (UFDR) files were not processed (over 100GB). (FCR-1254)
11. Resolved an issue where the changes made to the list of columns in the 'Overview' tab were updated back to default when an update was made in the file list. (FCR-599)
12. Resolved an issue where files from compressed New Technology File System (NTFS) drives were not processed (FCR-221)
13. Resolved an issue where the Map Drive option failed when trying to map remote drive for processing (FCR-1823)
14. Resolved an issue in FTK where processing was stuck in progress at the Database optimization stage when the 'Deduplication Analysis' option was enabled. (FCR-819)
15. Resolved an issue where the Entire Directory node was not displayed while adding a trusted user, especially on Microsoft Azure or Amazon S3 instances. (FCR-525)
16. Resolved an issue where cases were created in the shared ADG database, instead of their own database. (FCR-1185)



17. Resolved an issue where upon performing the export to image operation, the L01 segments were created at the C: Drive instead of creating in the specified location (FCR-2075)
18. Resolved an issue where adding a physical drive would cause the application to crash. (FCR-1289)
19. Resolved an issue where the 'Column set' dropdown within the File List panel disappears upon mouse-up. (FCR-1134)
20. Resolved an issue in System Summary where Invalid Creation, Last Access, Last Write date/time was shown against some items of Link and Shell Bags. (FCR-1157)
21. Resolved an issue where the Email bodies were displayed sporadically in the viewer. (FCR-1215)
22. Resolved an issue where the user was unable to delete cases from the RDS DB instances. (FCR-1171)
23. Resolved an issue where the root site server would intermittently stop replicating jobs to the public site server until the root site server was restarted. (FCR-1341)
24. Resolved an issue where EXIF data reflected the processing time of the artifacts and not the metadata of the artifact. (FCR-2031)
25. Resolved an issue where windows agents were unable to process windows.info during volatility memory analysis. (FCR-1802)
26. Resolved an issue where indexing options were not inherited from initial case processing options to additional analysis options. (FCR-1346)
27. Resolved an issue where artifacts in the internet/email tabs would utilize the normal column set, rather than the column sets directly associated with internet/email. (FCR-709)
28. Resolved the issue in the 'Language Translation' process while translating the content of chat files from German to English. (FCR-2787)



3 Known Issues

1. Project Vic hash sets and groups cannot be deleted within the FTK interface. (FCR-2070)
2. While exporting L01 image file types, the export operation's progress statistics are not displayed. (FCR-2409)
3. While exporting images as L01 file types, the image does not export in 1.5GB segments consistently. (FCR-2411)
4. When setting a Quin-C server in FTK preferences, using HTTPS within FTK "Preferences" does not change the ADGWeblabSelfHost configuration value to true (FCR-1233).
5. While processing the VMDK and VHDX files with the 'contents of a folder' option enabled, the corresponding files are not expanded and displayed. (FCR-2155).
6. Registry Summary Reports are not being created when selected as a processing option (FCR-1333).
7. During MBOX analysis, email attachments do not relate accurately to its related filetype panel when using the "View Item in Different List" option. (FCR-2686)
8. HEIC Conversions available within processing options, may sporadically fail over some files. (FCR-21)
Workaround: If a HEIC image has failed to process, use "Additional Analysis" to reprocess the image.
9. Files which are being viewed in the Mobile tab are not found in the Overview tab when using the "View Item in Different List" option. (FCR-2714)



Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:**Exterro, Inc.**

4145 SW Watson Ave., Suite 400

Beaverton, OR 97005.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail: info@exterro.com

Website: www.exterro.com

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation ("Trademarks") are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc's prior written consent. In addition, you may not use the